(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 November 2002 (21.11.2002)

PCT

(10) International Publication Number
WO 02/093823 A1

(51) International Patent Classification[7]: H04L 9/00, H04K 1/00

(21) International Application Number: PCT/US02/15187

(22) International Filing Date: 14 May 2002 (14.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/858,189 14 May 2001 (14.05.2001) US

(71) Applicant *(for all designated States except US)*: **DIGIMARC CORPORATION** [US/US]; 19801 SW 72nd Avenue, Suite 100, Tualatin, OR 97062 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RHOADS, Geoffrey, B.** [US/US]; 2961 SW Turner Road, West Linn, OR 97068 (US). **LEVY, Kenneth, L.** [US/US]; 110 NE Cedar Street, Stevenson, WA 98648 (US).

(74) Agent: **CONWELL, William, Y.**; Digimarc Corporation, 19801 SW 72nd Avenue, Suite 100, Tualatin, OR 97062 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/093823 A1

(54) Title: CONTENT IDENTIFIERS TRIGGERING CORRESPONDING RESPONSES

(57) Abstract: Fingerprint data derived from audio or other content is used as an identifier, to trigger machine responses corresponding to the content. The fingerprint can be derived from the content, and also separately encoded in a file header. Digital watermarks can also be similarly used.

CONTENT IDENTIFIERS TRIGGERING CORRESPONDING RESPONSES

Related Application Data

In the US, this application is a continuation in part of application 09/571,422, which claimed priority from applications 09/314,648, 09/342,688, 09/342,689, 09/342,971, 09/343,101, 09/343,104, 60/141,468, 60/151,586, 60/158,015, 60/163,332, 60/164,619, 09/531,076, 09/543,125, 09/547,664, and 09/552,998.

This application is also a continuation-in-part of copending applications 09/574,726 and 09/476,686, both of which claim priority to application 60/134,782.

The present application claims priority benefit to the foregoing applications.

The subject matter of this application is also related to that of 09/620,019, 60/257,822, 60/232,163, and 09/404,291.

Field of the Invention

The present invention relates to computer-based systems, and more particularly relates to systems that identify electronic or physical objects (e.g., audio, printed documents, video, etc.), and trigger corresponding responses.

Background

In application 09/571,422 (now laid-open as PCT publication WO 00/70585), the present assignee described technology that can sense an object identifier from a physical or electronic object, and trigger a corresponding computer response.

In applications 09/574,726 and 09/476,686, the present assignee described technology that uses a microphone to sense audio sounds, determine an identifier corresponding to the audio, and then trigger a corresponding response.

Detailed Description

Although the cited patent applications focused on use of digital watermarks to identify the subject objects/audio, they noted that the same applications and benefits can be provided with other identification technologies.

One such suitable technology - variously known as robust hashing, fingerprinting, etc. – involves generating an identifier from attributes of the content. This identifier can then be looked-up in a database (or other data structure) to determine

the song (or other audio track) to which it corresponds.

Various fingerprinting technologies are known. For example, a software program called TRM, from Relatable Software, was written up in the Washington Post as follows:

> *TRM performs a small technological miracle: It "fingerprints" songs, analyzing beat and tempo to generate a unique digital identifier. Since every song is slightly different, no two "acoustic fingerprints" are alike, not even live and studio versions of the same melody.*

Tuneprint is another such audio fingerprinting tool. Tuneprint is understood to utilize a model of human hearing used to predict how audio will appear after it's been distorted by the human ear, and the parts of neural processing that are understood. This is some of the same information that led to MP3 encoders achieving exceptional audio compression. Characteristics that uniquely identify the track are then identified by picking out the most important, surprising, or significant features of the sound.

Yet another fingerprinting program is Songprint, available as an open source library from freetantrum.org.

One form of fingerprint may be derived by applying content – in whole or part, and represented in time- or frequency format – to a neural network, such as a Kohonen self-organizing map. For example, a song may be identified by feeding the first 30 seconds of audio, with 20 millisecond fourier transformed windows, into a Kohonen network having 64 outputs. The 64 outputs can, themselves, form the fingerprint, or they can be further processed to yield the fingerprint.

A variety of other fingerprinting tools and techniques are known to artisans in the field. Others are disclosed, e.g., in applications 60/257,822, 09/563,664, and 09/578,551. See also the chapter on Fingerprinting by John Hyeon Lee, in Information Hiding: Techniques for Steganography and Digital Watermarking edited by Stefan Katzenbeisse and Fabien A.P. Petitcolas, published by Artech House.

One way to generate a fingerprint is to "hash" the audio, to derive a shorter code that is dependent, in a predetermined way, on the audio data. However, slight differences in the audio data (such as sampling rate) can cause two versions of the same song to yield two different hash codes. While this outcome is advantageous in certain outcomes, it is disadvantageous in many others.

Generally preferable are audio fingerprinting techniques that yield the same fingerprints, even if the audio data are slightly different. Thus, a song sampled at a 96K bitrate desirably should yield the same fingerprint as the same song sampled at 128K. Likewise, a song embedded with steganographic watermark data should generally yield the same fingerprint as the same song without embedded watermark data.

One way to do this is to employ a hash function that is insensitive to certain changes in the input data. Thus, two audio tracks that are acoustically similar will hash to the same code, notwithstanding the fact that individual bits are different. A variety of such hashing techniques are known.

Another approach does not rely on "hashing" of the audio data bits. Instead, the audio is decomposed into elements having greater or lesser perceptibility. Audio compression techniques employ such decomposition methods, and discard the elements that are essentially imperceptible. In fingerprinting, these elements can also be disregarded, and the "fingerprint" taken from the acoustically significant portions of the audio (e.g., the most significant coefficients after transformation of the audio into a transform domain, such as DCT).

Some fingerprinting techniques do not rely on the absolute audio data (or transformed data) per se, but rather rely on the changes in such data from sample to sample (or coefficient to coefficient) as an identifying hallmark of the audio.

Some fingerprinting algorithms consider the entire audio track (e.g., 3 minutes). Others work on much shorter windows – a few seconds, or fractions of seconds. The former technique yields a single fingerprint for the track. The latter yields plural fingerprints – one from each excerpt. (The latter fingerprints can be concatenated, or otherwise combined, to yield a master fingerprint for the entire audio track.) For compressed audio, one convenient unit from which excerpts can be formed is the frame or window used in the compression algorithm (e.g., the excerpt can be one frame, five frames, etc.).

One advantage to the excerpt-based techniques is that a song can be correctly identified even if it is truncated. Moreover, the technique is well suited for use with streaming media (in which the entire song data is typically not available all at once as a single file).

In database look-up systems employing fingerprints from short excerpts, a first fingerprint may be found to match 10 songs. To resolve this ambiguity, subsequent excerpt-fingerprints can be checked.

One way of making fingerprints "robust" against variations among similar tracks is to employ probabilistic methods using excerpt-based fingerprints. Consider the following, over-simplified, example:

Fingerprinted excerpt	Matches these songs in database
Fingerprint 1	A, B, C
Fingerprint 2	C, D, E
Fingerprint 3	B, D, F
Fingerprint 4	B, F, G

In this situation, it appears most probable that the fingerprints correspond to song B, since three of the four excerpt-fingerprints support such a conclusion. (Note that one of the excerpts - that which yielded Fingerprint 2 - does not match song B at all.)

More sophisticated probabilistic techniques, of course, can be used.

Once a song has been identified in a database, a number of different responses can be triggered. One is to impose a set of usage controls corresponding to terms set by the copyright holder (e.g., play control limitations, record control, fee charges, etc.) Another is to identify metadata related to the song, and provide the metadata to a user (or a link to the metadata). In some such applications, the song is simply identified by title and artist, and this information is returned to the user, e.g., by email, instant messaging, etc. With this information, the user can be given an option to purchase the music in CD or electronic form, purchase related materials (t-shirts, concert tickets), etc. A great variety of other content-triggered actions are disclosed in the cited applications.

One of the advantages of fingerprint-based content identification systems is that they do not require any alteration to the content. Thus, recordings made 50 years ago can be fingerprinted, and identified through such techniques.

Going forward, there are various advantages to encoding the content with the fingerprint. Thus, for example, a fingerprint identifier derived from a song can be stored in a file header of a file containing that song. (MP3 files, MPEG files, and most

other common content file formats include header fields in which such information can readily be stored.) The fingerprint can then obtained in two different ways – by reading the header info, and by computation from the audio information. This redundancy offers several advantages. One aids security. If a file has a header-stored fingerprint that does not match a fingerprint derived from the file contents, something is amiss – the file may be destructive (e.g., a bomb or virus), or the file structure may mis-identify the file contents.

In some embodiments, the fingerprint data (or watermark data) stored in the header may be encrypted, and/or authenticated by a digital signature such as a complete hash, or a few check bits or CRC bits. In such cases, the header data can be the primary source of the fingerprint (watermark) information, with the file contents being processed to re-derive the fingerprint (watermark) only if authentication of the fingerprint stored in the header fails. Instead of including the fingerprint in the header, the header can include an electronic address or pointer data indicating another location (e.g., a URL or database record) at which the fingerprint data is stored. Again, this information may be secured using known techniques.

Similarly, the fingerprint can point to a database that contains one or more IDs that are added via a watermark. This is useful when CDs are being converted to MP3 files (i.e. ripped) and the fingerprint is calculated from a hash of the table of contents (TOC) such as done with CDDB.com, or from all of the songs. In this case, the database entry for that fingerprint could include a list of IDs for each song, and these IDs are added via a watermark and/or frame header data. This can also be useful where the content is identified based upon a group of fingerprints from plural excerpts, in which case the database that determines the content also contains an identifier, unrelated to the fingerprint(s) for that piece of content that can be embedded via a watermark.

Instead of, or in addition to, storing a fingerprint in a file header, the fingerprint data may be steganographically encoded into the file contents itself, using known watermarking techniques (e.g., those disclosed in application 09/503,881, and patents 6,061,793, 6,005,501 and 5,940,135). For example, the fingerprint ID can be duplicated in the data embedded via a watermark.

In some arrangements, a watermark can convey a fingerprint, and auxiliary data as well. The file header can also convey the fingerprint, and the auxiliary data. And

even if the file contents are separated from the header, and the watermark is corrupted or otherwise lost, the fingerprint can still be recovered from the content. In some cases, the lost auxiliary data can alternatively be obtained from information in a database record identified by the fingerprint (e.g., the auxiliary information can be literally stored in the record, or the record can point to another source where the information is stored).

Instead of especially processing a content file for the purpose of encoding fingerprint data, this action can be done automatically each time certain applications process the content for other purposes. For example, a rendering application (such as an MP3 player or MPEG viewer), a compression program, an operating system file management program, or other-purposed software, can calculate the fingerprint from the content, and encode the content with that information (e.g., using header data, or digital watermarking). It does this while the file is being processed for another purpose, e.g., taking advantage of the file's copying into a processing system's RAM memory, from slower storage.

In formats in which content is segregated into portions, such as MP3 frames, a fingerprint can be calculated for, and encoded in association with, each portion. Such fingerprints can later be cross-checked against fingerprint data calculated from the content information, e.g., to confirm delivery of paid-for content. Such fingerprints may be encrypted and locked to the content, as contemplated in application 09/620,019.

In addition, in this frame based systems, the fingerprint data and/or watermark data can be embedded with some or all data throughout each frames. This way a streaming system can use the header to first check the song for identification, and if that identification is absent or not authenticated, the system can check for the watermark and/or calculate the fingerprint. This improves the efficiency and cost of the detecting system.

Before being encrypted and digitally signed, the data in the frame header can be modified by the content, possibly a hash of the content or a few critical bits of content. Thus, the frame header data cannot be transferred between content. When reading the data, it must be modified by the inverse transform of the earlier modification. This system can be applied whether the data is embedded throughout each frame or all in a global file header and is discussed in application serial 09/404,291 entitled "Method And Apparatus For Robust Embedded Data" by Ken Levy on 9/23/99. Reading this

secure header data is only slightly more complex than without the modification, such that the system is more efficient than always having to calculate the fingerprint and/or detect the watermark.

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the patents and patent applications cited above. It is applicant's express intention to teach that the methods detailed herein are applicable in connection with the technologies and applications detailed in these cited patents and applications.

Although the foregoing specification has focused on audio applications, it will be recognized that the same principles are likewise applicable with other forms of content, including still imagery, motion pictures, video, etc. Thus, for example, Digimarc MediaBridge linking from objects to corresponding internet resources can be based on identifiers derived from captured image data or the like, rather than from embedded watermarks. As such, the technique is applicable to images and video.

WE CLAIM:

1. A method comprising:

obtaining fingerprint data from a file header associated with a file, the fingerprint data being associated with contents of the file;

checking the integrity of the fingerprint data;

if the check leaves doubt about the fingerprint data thus obtained, then recalculating fingerprint data from contents of the file; and

transmitting the fingerprint data to a database.

2. The method of claim 1 that includes:

accessing a database record corresponding to the transmitted fingerprint data, to obtain associated information; and

returning at least some of said associated information to a computer device from which the fingerprint data was transmitted.

3. The method of claim 1 in which the file contents comprise audio.

4. The method of claim 1 in which checking includes checking a digital signature.

5. The method of claim 1 in which the checking includes decrypting fingerprint data from the header and authenticating the decrypted data.

6. The method of claim 5 that includes applying an inverse modification to the fingerprint in the header prior to said decrypting.

7. The method of claim 1 that includes applying an inverse modification to the fingerprint in the header.

8. A method comprising:

obtaining watermark data from a file header associated with a file, the watermark data being associated with contents of the file;

checking the integrity of the watermark data;

if the check leaves doubt about the watermark data thus obtained, then detecting watermark data from contents of the file; and

transmitting the watermark data to a database.

9. The method of claim 8 that includes:

accessing a database record corresponding to the transmitted watermark data, to obtain associated information; and

returning at least some of said associated information to a computer device from which the watermark data was transmitted.

10. The method of claim 8 in which the file contents comprise audio.

11. The method of claim 8 in which checking includes checking a digital signature.

12. The method of claim 8 in which the checking includes decrypting watermark data from the header and authenticating the decrypted data.

13. The method of claim 12 that includes applying an inverse modification to the watermark in the header prior to said decrypting.

14. The method of claim 12 that includes applying an inverse modification to the watermark in the header.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/15187

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 9/00; H04K 1/00
US CL : 713/170,176,186,189; 380/217; 382/115,116,124
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/170,176,186,189; 380/217; 382/115,116,124

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,037,984 A(ISNARDI et al.) 14 March 2000, col.2,lines 58-67, col.3,lines 1-9.	1-14
Y	US 6,061,451 A(MURATANI et al.) 09 May 2000, col.22,lines 25-28,56-67,col.23,lines 31-37, col.24,lines 35-50.	1-14.
A	US 5,915,027 A(COX et al.) 22 June 1999, col.5,lines 10-34, col.9,lines 21-60.	1-14
A	US 5,418,965 A(MAHAR et al.) 23 May 1995, col.15,lines 35-53, col.16,lines 20-58.	1-14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priorit date and not in conflict with the application but cited to understan the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot b considered novel or cannot be considered to involve an inventive ste when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot b considered to involve an inventive step when the document combined with one or more other such documents, such combinatic being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 27 JUNE 2002	Date of mailing of the international search report 02 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Peggy Harrod Telephone No. (703) 305-0042

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/15187

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

STN, EAST
search terms: digital signature,watermark,hash,header,fingerprint.biometric,message digest,authentication,MPEG,audio,media